Intelligent Frame Retention and Anomaly Detection with Notification Using YOLOv11m

Prajwal Patil, Mansi Subhedar*,
Prathmesh Shelke and Rohit Rakshe

Department of Electronics and Computer Science, Pillai HOC College of Engineering and Technology, Rasayani, Tal. Khalapur, Dist. Raigad, Maharashtra, India
E-mail: mansissubhedar@gmail.com
**Corresponding Author*

Received 12 March 2025; Accepted 07 April 2026

Abstract

This study aims to solve the problem of video storage and improves the overall efficiency of cameras by adopting real-time anomaly detection, hence informing the user about any suspicious anomalies. The proposed trained model processes live video streams, identifying unusual events and anomalies such as theft, weapons, or violent activities. Simultaneously, a video storage optimization algorithm reduces redundant frames while maintaining movement detected video streams from CCTV surveillance. In addition, if the model detects an unusual event occurring in the live video stream, it immediately notifies the user about the type of anomaly and the location of the event that occurred. Experimental results demonstrate that the proposed system effectively detects anomalies with an average

Journal of Mobile Multimedia, Vol. 22_2, 175–196.
doi: 10.13052/jmm1550-4646.2221

precision–recall score of 0.958 and an F1 confidence score of 0.93, ensuring reliable threat identification and detection. The model is robust and differentiates between normal and anomalous activities as justified by experimental results.

Keywords: Crime detection, deep learning, video storage optimization, real-time anomaly detection, security monitoring.

1 Introduction

Today, crime rates are increasing day by day in many areas around the world, and most crimes occur during the night when everyone is asleep. Even with the technology of smart CCTV surveillance, cameras have to constantly be monitored for suspicious activity which requires more human effort [1, 2]. In addition, live CCTV cameras record every minute of the day and the recorded stream of frames is temporarily saved for around a month [3, 4], hence, requiring more cost and storage requirements for storing roughly 720 hours of video data. However, finding a particular event that occurred in a particular 24 hour period could be challenging and inefficient [5]. In response to the growing need for improved security measures, more advanced monitoring systems than conventional CCTV installations have been developed [6]. This study presents an intelligent smart CCTV surveillance to address these issues by employing a convolution neural network (CNN) model for realtime anomalous detection while simultaneously optimizing video frames with messaging alerts. Video size can be optimized by removing redundant video frames and scaling the footage to achieve high-resolution output video [7].

CCTV records live video streams and feed them to the model in parts of one hour, that is, the camera records the first hour and it feeds to the model after that the model starts detecting anomalies and motions within the frames in the hour recorded. While this processing takes place, the CCTV further records another hour for feeding the model again. By the time the camera records its one hour, the model is available for processing its next hour. The proposed model can notify the user when the model detects any anomaly or unusual activity. The remainder of this paper is organized as follows. Section 2 presents an overview of real-time anomaly detection and video storage optimization related studies. The proposed methodology is presented in Section 3. Section 4 discusses data flow diagram. Simulation results are discussed in Section 5. Section 6 concludes the proposed work.

2 Related Study

The advancement of video surveillance technology has been profoundly shaped by developments in artificial intelligence and deep learning, resulting in enhanced security protocols and improved capabilities for detecting anomalies. The implementation of real time monitoring and automated alert systems has fortified security frameworks, facilitating prompt response to potential threats. Ali et al. proposed a real time anomaly detection system aimed at improving the efficiency of surveillance by recognizing threats as they arise [1]. This system processes video feeds in real time, enabling security personnel to act without delay. Singh et al. investigated the use of neural networks for identifying anomalies in CCTV footage, offering a methodology that enhances security monitoring through sophisticated detection techniques, thereby minimizing false alarms and boosting reliability [2]]. The effective management of surveillance data is essential given the growing volume of recorded footage. Western Digital outlined methods for optimizing CCTV storage, concentrating on the efficient management and deletion of footage while adhering to data retention regulations [4]. Storage efficiency is vital for sustaining scalable and cost-effective surveillance operations.

The dependability of anomaly detection in diverse environmental conditions continues to pose challenges. Leroux et al. created a multi-branch neural network aimed at identifying anomalies under challenging lighting and weather conditions [5]. Their strategy guarantees reliable detection despite external factors that could impair video quality. Rahman et al. analyzed the significance of smart CCTV within urban security frameworks, highlighting the critical role of intelligent surveillance solutions in improving public safety while tackling issues related to data management and implementation [6]. Arora et al. put forward optimization strategies aimed at reducing video redundancy while maintaining essential surveillance footage [7]. Their research presents advanced compression techniques that focus on preserving important segments of video and discarding superfluous frames, thereby optimizing storage efficiency. The inclusion of datasets is crucial for enhancing anomaly detection models. The Anomaly Detection Dataset serves as a vital resource for the training and assessment of surveillance algorithms, contributing to improved accuracy and performance [8]. Furthermore, Google Colab provides a collaborative environment for the training of deep learning models, enabling researchers to explore various neural architectures and bolster detection capabilities [9].

The significance of IoT-enabled surveillance systems has grown markedly in high-security settings. Afreen et al. unveiled an IoT-driven smart surveillance system that improves real-time threat detection and response strategies, illustrating the efficacy of interconnected devices in monitoring security footage [10]. Ahmed et al. concentrated on deep learning techniques for weapon detection in CCTV footage, achieving notable accuracy in threat identification and proactive security measures [11]. Real-time object detection is critical for ensuring public safety in urban areas. Ingle et al. created an anomaly detection system for smart cities that integrates computer vision and deep learning to scrutinize movement patterns and identify atypical activities [12]. Jeon et al. presented PASS-CCTV, a framework tailored for challenging environmental conditions, guaranteeing dependable surveillance monitoring [13]. Manu et al. proposed an anomaly alert system that incorporates automated notifications within CCTV networks, facilitating prompt responses to identified threats. Automated alert systems are essential for proactive monitoring [14]. Shukla et al. developed a system that generates real-time notifications upon detecting security threats in video streams, thereby minimizing the necessity for continuous human oversight [15]. Tatiya et al. improved the accuracy of anomaly detection through the application of deep learning methods, which significantly decreased response times and enhanced overall security measures [16].

The existence of real-world datasets has been instrumental in creating more effective anomaly detection models. The University of Central Florida offers a widely recognized benchmark dataset for surveillance research, aiding in the evaluation and enhancement of models [17]. Wang et al. introduced a real-time camera anomaly detection framework that proves to be highly effective in practical scenarios [18]. Zhou et al. developed AnomalyNet, a dedicated neural network model for video-based anomaly detection, which optimizes computational efficiency while maintaining accuracy [19]. Sultani et al. utilized extensive datasets to refine detection models, enabling ongoing learning and adaptation to changing security threats [20]. Together, these studies underscore the progress made in intelligent surveillance systems, particularly in the areas of anomaly detection and storage Internet of Things (IoT), and real-world datasets continue to foster innovation in automated surveillance, enhancing the efficiency, scalability, and responsiveness of security systems. Future research is expected to focus on improving detection accuracy, minimizing computational demands, and enhancing the interoperability of surveillance networks with emergency response teams.

3 Methodology

This study has multiple sections of development, including real-time anomaly detection, instantaneous optimization of the real-time video frames inspired by [1, 2, 7], and messaging alerts to users. It is done by sending the output of the live camera, which is a continuous stream of frames, to the model input. The methodology follows a structured approach, beginning with video capture, followed by frame extraction, frame selection based on a statistical threshold, anomaly detection using a trained model and immediately notifying the user if any anomaly is detected. The system architecture is built to handle real-time video data, ensuring that any anomalies detected are reported to users instantly, enabling instant action. This section outlines the key algorithm and technique employed in the development of the proposed system.

3.1 Real-time Anomaly Detection

The system does not process every frame it records directly. Instead, a separate video storage optimizer algorithm optimizes the video stream before sending the optimized frames to the anomaly detection model. This approach ensures that the system operates efficiently without being overwhelmed by continuous frames of video data. Initially, the system temporarily stores the first hour of recorded footage, aligning with the video optimization process to manage data effectively. A frame counter is then set to zero to keep track of the sequence of frames. As new frames are captured, the counter increases by one with each frame. The flow of the real-time anomaly detection process is shown in Figure 1. Instead of processing every frame, a filtering condition is applied: only frames where the counter value is a multiple of 20 (such as 20, 40, 60, etc.) are selected and sent to the trained anomaly detection model for analysis and processing. This method significantly reduces the number of frames the model needs to process, optimizing computational efficiency while maintaining high accuracy in detecting unusual activities. If a frame does not meet the selection criteria, it is simply skipped, and the counter continues to increment. By using this selective sampling method, the system prevents excessive processing of consecutive frames, which helps conserve resources while still ensuring that critical moments are analyzed for anomalies. Once an anomaly is detected, the system immediately updates the real-time user interface, alerting the concerned user through instant notifications.

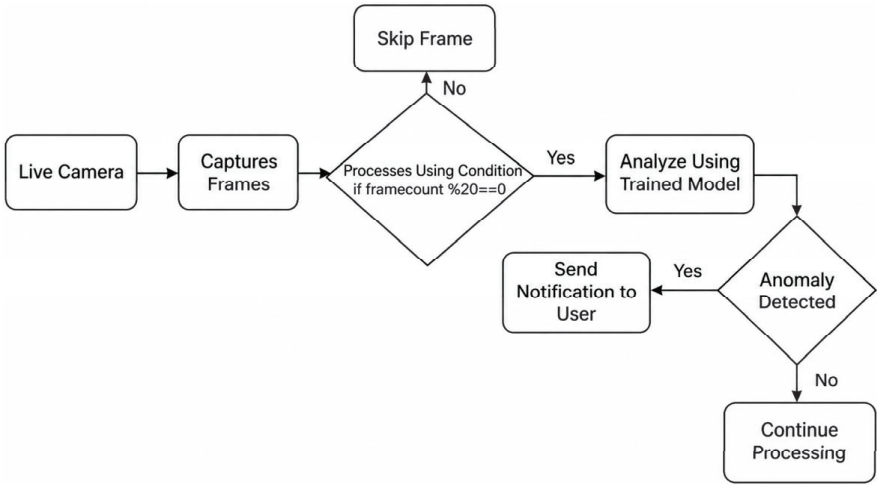

Figure 1 The proposed method.

3.2 Video Storage Optimization Algorithm

It has never been easy to handle the large volume of video data produced by CCTV cameras. Because these cameras record continually, they require more storage over time, which makes resource management challenging. The majority of CCTV systems retain recordings for approximately 30 to 31 days [4], resulting in a substantial storage requirement. However, by processing the recorded film while maintaining its crucial features, this storage burden can be significantly decreased. This study focuses on solving the same issue by using an optimization technique based on the mean squared error (MSE) method, inspired by [7]. This method not only helps in reducing storage space but also enhances the quality of the recorded frames. The approach is efficient because it ensures that unnecessary data is removed while maintaining the overall features of the recorded video. The MSE based optimization is less time consuming although highly effective for processing continuous video streams.

The video storage optimization process starts with the system constantly capturing video frames in real time. Instead of handling an entire day's footage at once, the recording is divided into one-hour segments. While one hour of video is being processed, the next hour is recorded simultaneously. Once recorded, the MSE algorithm analyzes it. The algorithm compares each frame with the next one to measure how different they are. If the difference between two frames (MSE value) is above a certain threshold, it means there is a meaningful change, so the frame is saved. On the other hand, if

the difference is minimal, the frame is discarded to eliminate redundancy. This selective approach helps in significantly reducing the video file size without affecting its essential details. After optimization, the retained frames are organized with accurate timestamps to maintain proper sequence. The bit rate of each frame is adjusted to ensure smooth video playback without compromising visual quality. Finally, all the optimized video segments are combined to recreate a complete video that takes up much less space while still maintaining a clear and detailed view.

3.3 Messaging Alert

When the system detects an anomaly, it immediately sends a real-time alert to the concerned user, ensuring that security personnel or relevant users are notified without delay. Each notification includes important information such as the exact timestamp of the detected anomaly and the classification of the object or activity involved in that anomaly. This additional data allows concerned users to understand the nature of the potential threat at a glance.

3.4 Dataset Used

This study uses a convolutional neural network (CNN) model that has been trained using different datasets containing incidents like accidents, robberies, fires, and other crimes. Because of this training, the model can accurately detect unusual activities in live CCTV footage. The system works by processing continuous incoming video frames from CCTV cameras. Firstly, it processes one hour of recorded footage while the camera continues recording the next hour. This method makes sure that there are no delays in detecting anomalies. Once the first hour of footage is processed, the model moves on to the next hour, making a cycle required for real-time processing. The major part of this system is the YOLO11m model, which has been trained using the Anomaly Detection Dataset. This fine-tuning helps the model quickly and correctly identify suspicious activities.

The datasets used for training, along with their details, are listed in Table 1, showing the different crime situations the system can recognize. The Anomaly Detection Dataset from Roboflow Universe has been used for training the model [21]. This dataset consists of annotated images capturing various criminal activities in real-world surveillance environments. It has been used to fine-tune the YOLO11m model for detection of anomalies. To maximize efficiency, the proposed model was trained for 70 epochs. Table 2 provides a detailed breakdown of the dataset, including the number of classes and the corresponding distribution of images for training, testing,

Table 1 Dataset and training configuration summary.

Attribute	Details
Dataset Overview	
Source	Roboflow Universe
Total classes	4 (fight, fire, accident and smoke)
Total images	10385 (train: 7567, validation: 1660, test: 1158)
Annotation format	Bounding boxes with class labels
Resolution	640×640 pixels
Diversity	Captured under varied lighting and environmental conditions
Model training configuration	
Pre-trained model	YOLO11m (COCO dataset)
Batch size	16
Epochs	70
Optimizer	Adam
Learning rate	10^{-3}, decayed to 10^{-4}
Loss function	Object detection loss (classification + localization + confidence)
Augmentation	Flipping, rotation, scaling, color adjustments

Table 2 Dataset class distribution.

Classes	Train	Valid	Test	Total
Fight	3145	889	461	4495
Fire	1534	434	220	2188
Smoke	1650	170	86	1906
Accident	1238	167	391	1796

and validation. The dataset has four classes, covering a range of anomalies such as weapons, regular movement, vehicles, accidents, and fire.

3.5 Integrated Architecture

After building individual sections and training the model as per objectives, every section is integrated along with the custom trained YOLO11m model. Integrated sections consist of real-time anomaly detection and video storage optimization, see Figure 2. The algorithm follows the following framework. Capture real-time video feed from CCTV cameras and store one hour of recorded footage before processing. The recorded footage is converted into frames for further analysis. The anomalies i.e. abnormal activities are identified using the custom trained YOLO11m model. It is followed by filtering and optimizing frames for storage efficiency. The selected frames are analyzed using the trained YOLO11m model and contextual information is extracted

such as timestamp and anomaly classification. If the anomaly is detected, a notification is automatically sent to the user through the UI and messaging system. For video optimization, the mean squared error (MSE) between consecutive frames is calculated and compared with a predefined threshold. If the MSE is below the threshold, the frame is considered to be redundant and will be deleted. If MSE meets or exceeds the threshold, the frame is considered to be significant and will be stored. The bit rate is adjusted to improve efficiency and optimize storage.

4 Data Flow Diagram

This data flow diagram (DFD) as depicted in Figure 2 illustrates a system designed for realtime video anomaly detection and storage optimization.

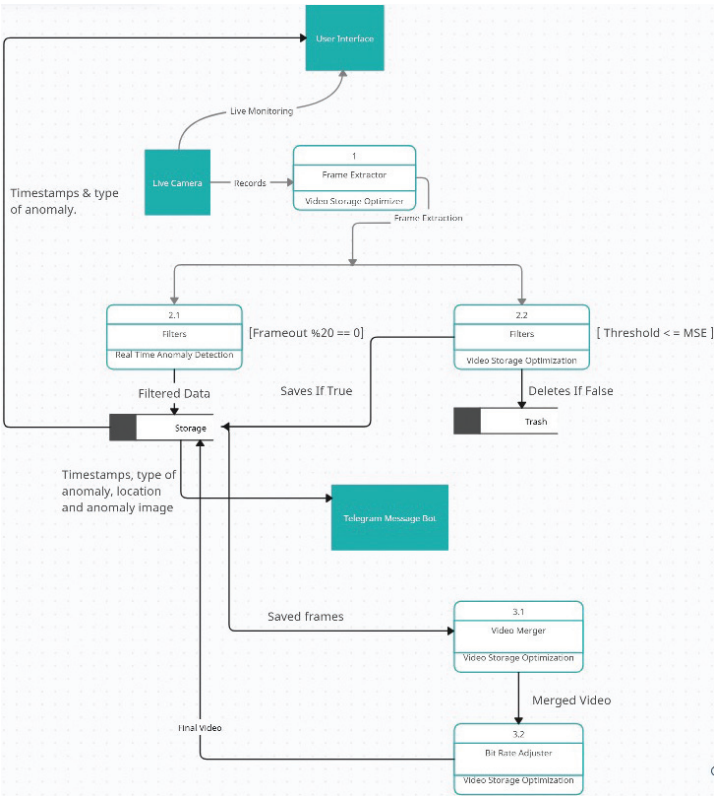

Figure 2 Data flow diagram.

A concise overview is: live camera captures and streams video for immediate surveillance and transmits frames for further analysis. The frame extraction module isolates frames from the recorded footage and enhances storage efficiency by selecting essential frames. Real-time anomaly detection examines frames for any irregularities. Upon detecting an anomaly, the frame is archived along with pertinent details (timestamp, type, location, image). Video storage optimization assesses frames against a predetermined threshold (mean squared error, MSE). The frames failing to meet the threshold criteria are removed. Storage and alerts archive significant data (timestamps, type, location, images of anomalies).

A Telegram Message Bot dispatches notifications containing details of the anomalies. Final video processing: video merger integrates saved frames into a cohesive final video. The bit rate adjuster refines the video size to enhance storage efficiency. To further substantiate the model's effectiveness, visual results depicting detections on test images were examined. These results include bounding boxes and confidence scores for various objects, such as weapons and suspicious behaviors.

4.1 Use Case Diagram

The use case diagram presented in Figure 3 illustrates a real-time video anomaly detection and alert system, which comprises several essential components.

1. Actors: The user engages in monitoring live recordings and receives alerts regarding anomalies. The security/police also oversees the system and is notified of anomalies for security-related purposes.
2. Use cases: Live recording captures video in real-time while incorporating functionality for anomaly detection. Real-time anomaly detection recognizes atypical behaviors and enhances video storage management. Video storage optimization facilitates effective storage by filtering out non-essential frames. The alert mechanism dispatches notifications that include details of the anomalies (such as messages, timestamps, and types of anomalies) to both users and security personnel.
3. Relationships: Both the user and security/police are actively monitoring the system. Anomaly detection contributes to the optimization of storage for improved efficiency. The alert mechanism informs both actors whenever an anomaly is identified.

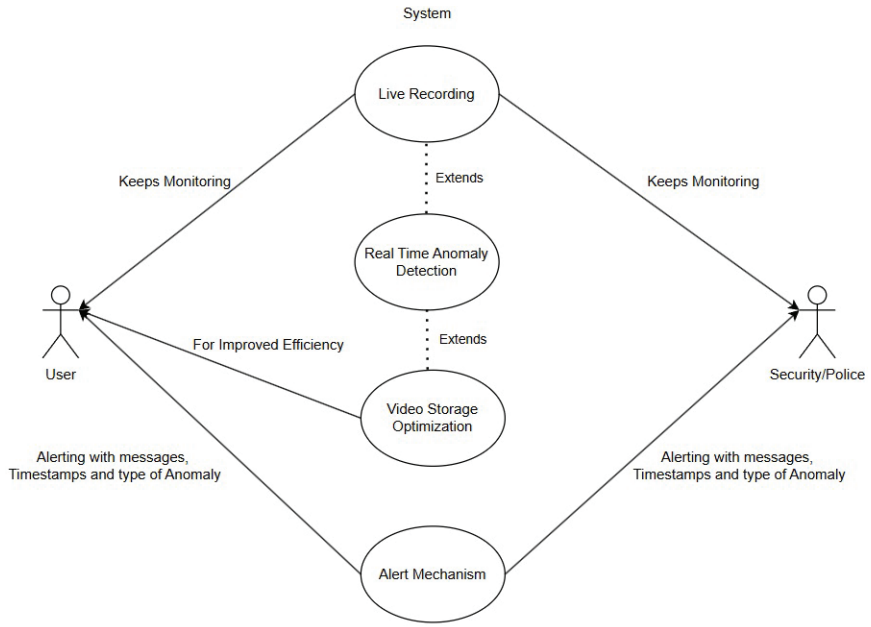

Figure 3 Use case diagram.

5 Simulation Results and Discussions

This section describes the experimental setup and the results obtained from real-time anomaly detection in CCTV surveillance. For the system to identify anomalous events, the model was trained and validated by the Roboflow dataset [18].

5.1 Experimental Setup

The setup includes a PC running a 64-bit Windows 11 operating system including an Intel Core i5-12500H CPU with Intel Iris Xe Graphics and 16 GB DDR4 RAM with base speed 2.5 GHz with 12 cores. The model was trained using the Google Colab Pro environment, which provides access to high-performance GPUs [9]. The training utilized the NVIDIA A100 GPU, featuring 40 GB of GPU memory, making it ideal for extensive deep learning applications. By utilizing Google Colab Pro, the training and evaluation processes were executed efficiently, leading to a substantial decrease in overall computational time. Figure 4 and Figure 5 exhibit sample images used in batches for training and validating the system model.

Figure 4 Training batch 1.

5.2 Results and Discussion

This section outlines the performance metrics of the fine-tuned YOLO11m model specifically tailored for applications in crime detection. As illustrated in Figure 6, the model achieved an average precision–recall curve of 0.958 and an average F1-confidence curve of 0.93, as seen in Figure 7. These results underscore the model's capability to effectively localize and classify objects within intricate scenarios. The images shown in Figures 8 and 9 illustrate the manner in which users engage with the anomaly detection system. The initial image presents the live video feed, enabling users to observe real-time

Figure 5 Validation batch 1.

footage with ease. The subsequent image showcases the alert mechanism in operation; upon detecting an anomaly, the system promptly transmits an alert message accompanied by an image of the incident. The buffer period is only for the backend video storage optimization part. The anomaly detection and alert system work in real time. The buffer is a backend optimization layer to reduce redundant video storage, compress and organize footage and store only relevant segments. This configuration guarantees that security personnel or users receive immediate notifications.These images shows how the system detects different types of threats in real-time using bounding boxes. Figure 10 shows the model identifying various accident scenarios. Figure 11 captures

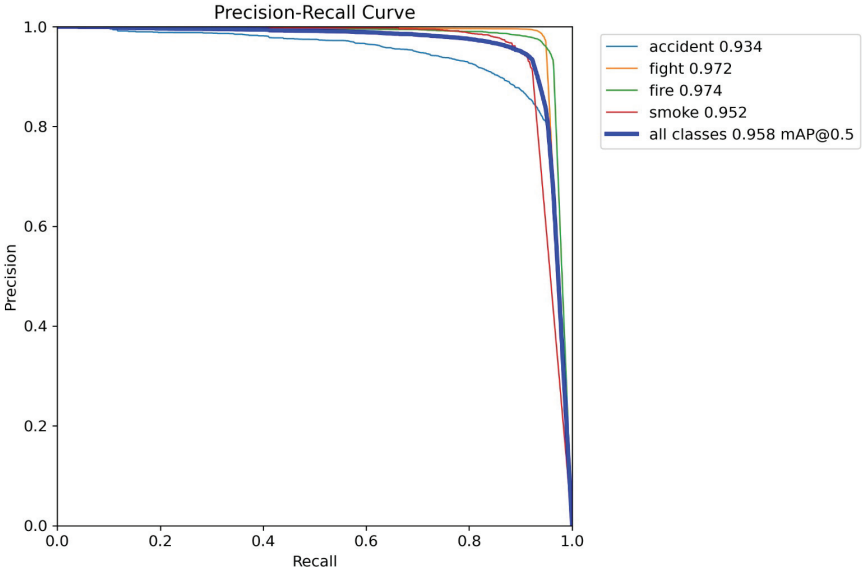

Figure 6 Precision–recall curve.

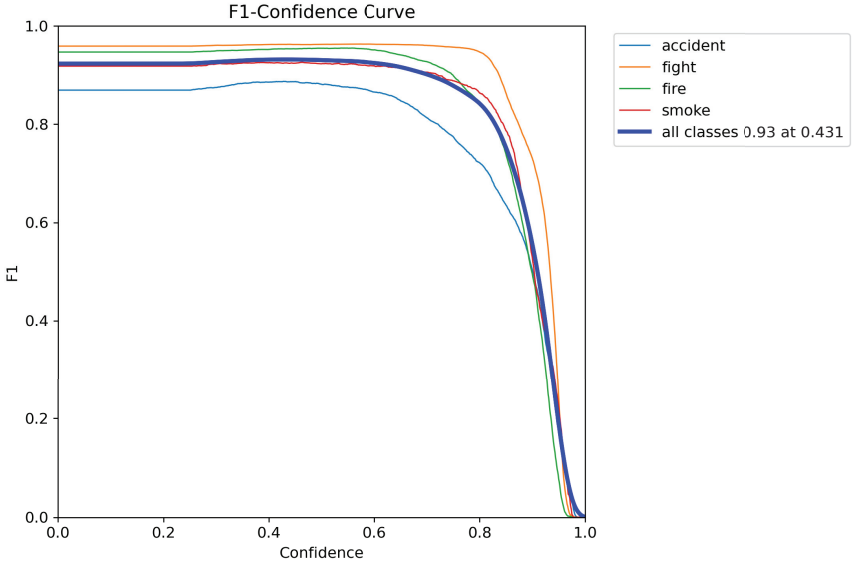

Figure 7 F1 confidence curve.

Table 3 Experimental results of system.

Sr. No.	Metric	Value	Significance
1	Dataset used	Anomaly detection dataset (Roboflow)	10,385 annotated images across 4 crime-related classes
2	Model architecture	YOLO11m	Optimized for real-time anomaly detection
3	Precision–recall score	0.958	High accuracy in identifying anomalies
4	F1 confidence score	0.93	Strong model reliability in classification
5	Storage optimization	Mean squared error (MSE)	Reduces redundant frames while maintaining video quality
6	Training epochs	70	Ensures model convergence and accuracy
7	Optimization algorithm	Adam optimizer	Enhances model learning and generalization
8	Hardware used	NVIDIA A100 GPU (40GB VRAM)	Enables efficient deep learning computations

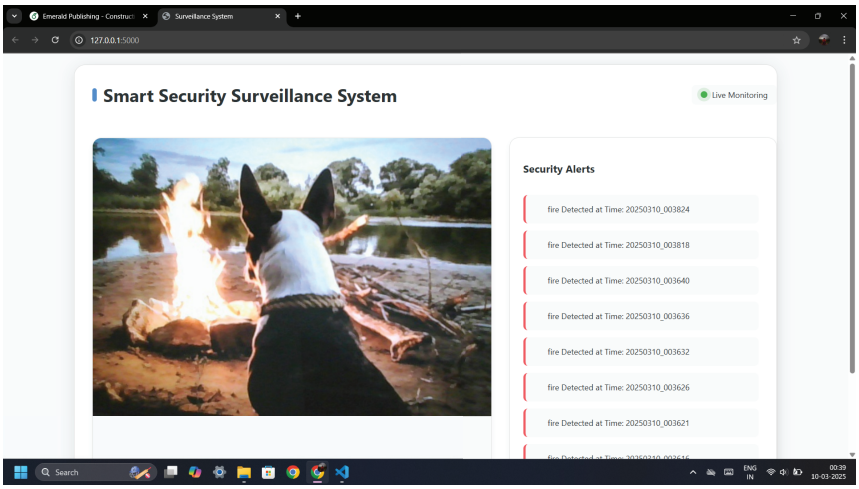

Figure 8 User interface with live video feed.

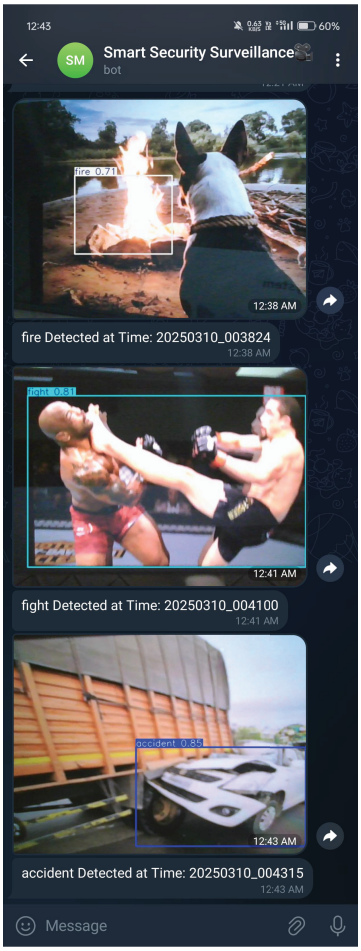

Figure 9 Chatbot notification.

smoke detection and fights, timely informing the user about the heated situation. Table 3 shows the performance of an anomaly detection system designed for real-time crime detection. Table 4 presents a comparison of the proposed work with similar existing works in literature. It uses the "Anomaly Detection Dataset" from Roboflow, which includes over 10,000 labeled images across 16 different crime-related categories. The model is built on YOLO11m, fine-tuned, and custom-trained on the dataset. It achieves a precision–recall score

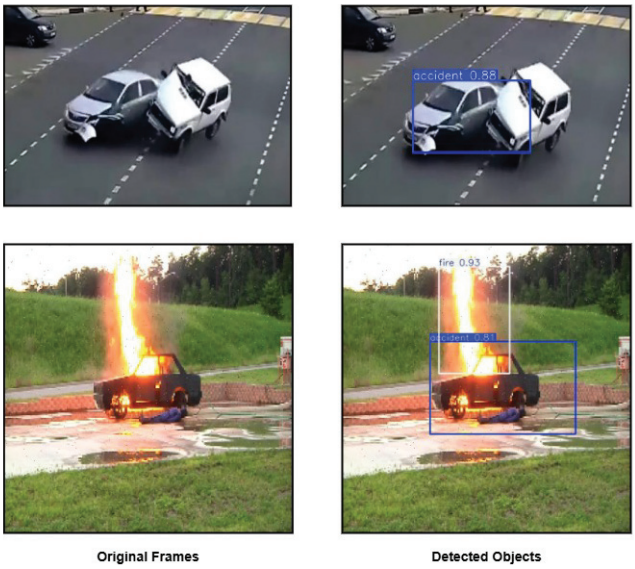

Figure 10 Detection of threats with bounding boxes.

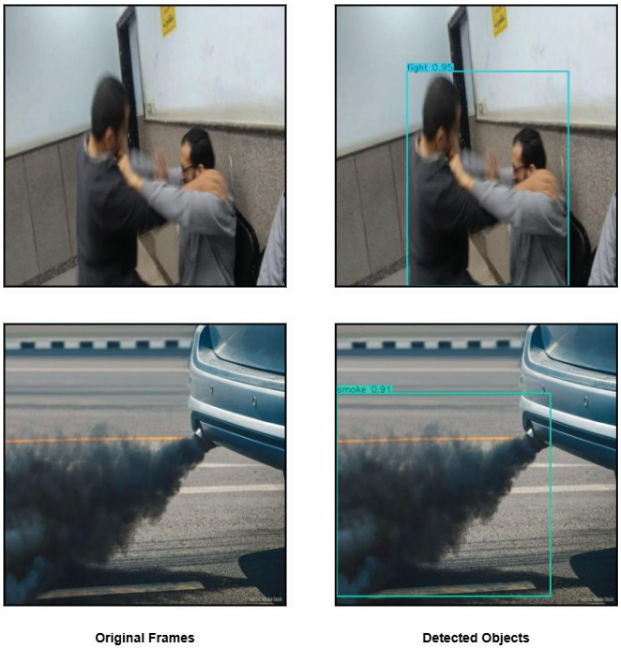

Figure 11 Detection of threats with bounding boxes.

Table 4 Comparison of proposed method with existing techniques.

Reference	Dataset	Technique	F1-Score
[1]	UCSD Ped1	Conv-AE + BS + Object Detection	91.8
[2]	UCF-Crime	CNN	0.9630
[20]	UCF-Crime	CNN	75.41
Proposed method	Crime detection	YOLOv11m	0.93

of 0.958 and an F1 confidence score of 0.93. To optimize storage, the system uses mean squared error (MSE) to remove unnecessary frames while keeping video quality intact. The training was conducted over 70 epochs using the Adam optimizer.

6 Conclusion

This work aims at improving real-time security monitoring while minimizing video storage expenses. Conventional CCTV systems face challenges related to excessive data generation and delayed anomaly detection resulting in elevated operational costs and inefficiencies. The proposed system addresses these issues by incorporating a finely-tuned YOLO11m deep learning model for anomaly detection alongside an MSE-based video optimization technique that selectively retains only pertinent frames. The system is capable of processing continuous video streams in real-time accurately identifying threats such as fights, fire, accidents, and smoke. The anomaly detection model was trained on the anomaly detection dataset from Roboflow Universe, which encompasses four crime-related categories and a total of 10,385 annotated images. The training was conducted over 70 epochs, utilizing an Adam optimizer, a batch size of 16, and a learning rate that decayed from 0.001 to 0.0001. Data augmentation methods, including random flipping, rotation, scaling, and color modifications were employed to enhance the model's generalization capabilities. Experimental assessments validate the efficacy of the proposed system in both anomaly detection and video storage optimization. The system achieved an average precision–recall score of 0.958 and an F1 confidence score of 0.93, underscoring its proficiency in reliably detecting security threats. Furthermore, the MSE-based optimization approach significantly reduces storage costs by eliminating redundant frames while maintaining critical surveillance footage.

References

[1] M. M. Ali, "Real-time video anomaly detection for smart surveillance," IET Image Process., Dec. 2022, doi: 10.1049/ipr2.12720.

[2] V. Singh, S. Singh, and P. Gupta, "Real-time anomaly recognition through CCTV using neural networks," Procedia Comput. Sci., vol. 173, pp. 254–263, 2020, doi: 10.1016/j.procs.2020.06.030.

[3] Fellows Research, "CCTV Surveillance Trends," 2021.

[4] Western Digital, "CCTV storage: Safely managing and deleting surveillance footage," Western Digital Blog. [Online]. Available: https://www.westerndigital.com/en-in/solutions/cctv/blog/cctv-storage-managing-deletingsurveillance-footage. Accessed: Jan. 7, 2025.

[5] S. Leroux, B. Li, and P. Simoens, "Multi-branch neural networks for video anomaly detection in adverse lighting and weather conditions," in Proc. IEEE/CVF Winter Conf. Appl. Comput. Vis. (WACV), Waikoloa, HI, USA, 2022, pp. 3027–3035, doi: 10.1109/WACV51458.2022.003086.

[6] M. F. B. A. Rahman, Smart CCTVs for Secure Cities: Potentials and Challenges,Policy Report. S. Rajaratnam School of International Studies, Nanyang Technological University, July 2017.

[7] S. Arora, K. Bhatia, and V. Amit, "Storage optimization of video surveillance from CCTV camera," in Proc. 2nd Int. Conf. Next Gen. Comput. Technol. (NGCT), 2016, doi: 10.1109/NGCT.2016.7877503.

[8] Roboflow, "Anomaly Detection Dataset," [Online]. Available: https://universe. roboflow.com/smartsurveillance/anomaly-2k9fc. Accessed: Feb. 7, 2025.

[9] Google, "Google Colaboratory," [Online]. Available: https://colab.research.google.com/. Accessed: Feb. 7, 2025.

[10] H. Afreen, M. Kashif, Q. Shaheen, Y. H. Alfaifi, and M. Ayaz, "IoT-Based Smart Surveillance System for High-Security Areas," Appl. Sci., vol. 13, no. 15, p. 8936, Aug. 2023, doi: 10.3390/app13158936.

[11] S. Ahmed, M. T. Bhatti, M. G. Khan, B. L¨ovstr¨om, and M. Shahid, "Development and optimization of deep learning models for weapon detection in surveillance videos," Appl. Sci., vol. 12, no. 12, p. 5772, June 2022, doi: 10.3390/app12125772.

[12] P. Y. Ingle and Y.-G. Kim, "Real-time abnormal object detection for video surveillance in smart cities," Sensors, vol. 22, no. 10, p. 3862, May 2022, doi: 10.3390/s22103862.

[13] H. Jeon, H. Kim, D. Kim, and J. Kim, "PASS-CCTV: Proactive Anomaly Surveillance System for CCTV Footage Analysis in Adverse Environmental Conditions," Expert Syst. Appl., vol. 254, p. 124391, Nov. 2024, doi: 10.1016/j.eswa.2024.124391.

[14] M. Y. M. Manu, R. G. K. Ravikumar, and S. S. V. Shashikala, "Anomaly alert system using CCTV surveillance," in Proc. IEEE 2nd Mysore Sub Sect. Int. Conf. (MysuruCon), Oct. 2022, doi: 10.1109/MysuruCon55714.2022.9972363.

[15] V. Shukla, G. K. Singh, and P. Shah, "Automatic alert of security threat through video surveillance system," in Proc. 54th Inst. Nucl. Mater. Manage. Annu. Meeting, Palm Desert, CA, USA, Jul. 2013.

[16] J. Tatiya, R. Makhija, M. Pathe, and S. Late, "Anomaly detection for video surveillance,"Int. J. Sci. Res. Sci. Technol., vol. 7, no. 3, pp. 1–5, May 2021, doi: 10.32628/IJSRSR21869.

[17] University of Central Florida, "Real-world dataset project," 2024. [Online]. Available: https://www.crcv.ucf.edu/projects/real-world/. Accessed: Oct. 20, 2024.

[18] Y.K. Wang, C.T. Fan, C. Y. Ke, and P. S. Deng, "Real-time camera anomaly detection for real world video surveillance," in Proc. Int. Conf. Mach. Learn. Cybern. (ICMLC), vol. 4, Aug. 2011, doi: 10.1109/ICMLC.2011.6017032.

[19] J. T. Zhou, J. Du, H. Zhu, and X. Peng, "AnomalyNet: An anomaly detection network for video surveillance," IEEE Trans. Inf. Forensics Security, vol. PP, no. 99, pp. 1–1, Feb. 2019, doi: 10.1109/TIFS.2019.2900907.

[20] W. Sultani, C. Chen, and M. Shah, "Real-world anomaly detection in surveillance videos," arXiv preprint arXiv:1801.04264, Jan. 2018, doi: 10.48550/arXiv.1801.04264.

[21] https://universe.roboflow.com/smartsurveillance/anomaly-2k9fc. [Accessed: Apr. 4, 2024]. https://universe.roboflow.com/smartsurveillance/anomaly-2k9fc. Accessed: Mar. 10, 2025.

Biographies

Prajwal Patil has obtained a B.Eng. in electronics and computer science from Pillai HOC College of Engineering and Technology. Currently he is working for Tata Consultancy Services.

Mansi Subhedar holds a Ph.D. in Electronics Engineering and has over 19 years of experience in teaching, research, and academic leadership. She is the Head of the Department of Electronics and Computer Science and IQAC Coordinator at Pillai HOC College of Engineering and Technology, Navi Mumbai. She has published 52 papers in peer-reviewed journals and conferences and serves as a reviewer for reputed publishers such as Elsevier, Springer, and Taylor & Francis. Dr. Subhedar is an approved PG and Ph.D. guide at the University of Mumbai and is a Senior Member of IEEE, Fellow of IETE, and Life Member of ISTE, IEI, and CSI. She has contributed to accreditation processes, mentored students in national competitions, and holds Six Sigma Green Belt certification. Her research interests include IoT, telecommunication networks, Industry 4.0, and machine learning. She is

also an active speaker, delivering expert sessions and hands-on training in emerging technologies.

Prathmesh Shelke has obtained a B.Eng. in electronics and computer science from Pillai HOC College of Engineering and Technology. Currently he is working with Quality Kiosk Technologies Pvt. Ltd.

Rohit Rakshe obtained a B.Eng. in electronics and computer science from Pillai HOC College of Engineering and Technology. Currently he is working with CognexiaAi.